Trendi informacijske varnosti v sodobni organizaciji

Kaja Prislan, Igor Bernik
Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana
kaja.prislan@fvv.uni-mb.si; igor.bernik@fvv.uni-mb.si

Izvleček

Trenutne gospodarske razmere in finančna kriza so z varnostnega, razvojnega in konkurenčnega vidika ustvarile neugodno izhodišče za vsako sodobno organizacijo. Kritična odvisnost operativnih ter taktičnih poslovnih ciljev od tehnologije povečuje organizacijske ranljivosti, tveganja in varnostne potrebe. Raziskave o stanju informacijske varnosti in kibernetskih grožnjah kažejo, da so organizacije neučinkovite pri sledenju varnostnim trendom ter neracionalne pri vzpostavljanju zaščite pred tveganji, ki jih prinaša najnovejša tehnologija. Ugotavljajo tudi, da je učinkovitost omenjene varnostne funkcije vse pogosteje povezana z netehničnimi upravljavskimi funkcijami. Ob predpostavki, da organizacije razpolagajo z osnovnimi tehničnimi rešitvami, so razvit varnostni menedžment, multidisciplinarni pristop, vodstveni odnos in ustrezna organizacijska kultura ključni dejavniki zanesljive in celovite informacijske varnosti.

Ključne besede: informacijska varnost, organizacije, učinkovitost, varnostni trendi, varnostni menedžment.

Abstract

Information Security Trends in a Modern Organisation

The current economic situation and the financial crisis have created an unfavourable starting point for any modern organisation in terms of their security, development and competitiveness. The critical dependence of their operational and tactical business goals on technology increases organisations' vulnerability, risks and security needs. Research studies focusing on information security situations and cyber threats demonstrate organisations' inefficiency in following security trends and their irrational decisions related to the adoption of protection measures against risks generated by the latest technology. These studies also find that the efficiency of security-related functions is ever more frequently linked to non-technical managerial functions. If one presumes that organisations have basic technical solutions at their disposal, it becomes obvious that well-developed security management, multidisciplinary approach, management's attitude and adequate organisational culture represent key factors for a reliable and comprehensive information security.

Key words: information security, organisations, efficiency, security trends, security management.

1 UVOD

Zadnje desetletje je zaznamovano z eksponentno integracijo informacijsko-komunikacijske tehnologije v vsakodnevno življenje razvitih družbenih struktur. Tehnološki napredek in njegove prednosti (npr. hitrejša komunikacija in stalen dostop do podatkov) so povzročili veliko odvisnost organizacij od nemotenega in zanesljivega delovanja informacijskih sistemov. Izpolnjevanje organizacijskih ciljev in doseganje konkurenčnosti v poslovnem okolju je vse pogosteje pogojeno z uporabo učinkovitih varnostnih rešitev na področju informacijske varnosti, saj informacijski sistemi v organizacijskih strukturah postajajo vse bolj kompleksen in integriran del delovnih (poslovnih) aktivnosti. So tudi temelj kibernetskega okolja, ki podpira shranjevanje, prenos in obdelavo zaupnih informacij. To pomeni, da je informacijsko-komunikacijska tehnologija znotraj organizacij razvila posebno okolje, ki je sestavljeno iz njihovega najpomembnejšega premoženja, hkrati pa omogoča zunanje in notranje vstope v virtualno organizacijsko strukturo. Z varnostnega vidika je to povzročilo nova tveganja.

Z zagotavljanjem učinkovite informacijske varnosti, ki prispeva k razvoju sodobne organizacije, so v praksi povezane številne dileme. Teoretično sicer obstajajo idealne okoliščine, v katerih so izvedeni vsi ustrezni postopki: varnostni menedžment je razvit in ozaveščen, tehnični oddelek je usposobljen in na voljo, zaposleni so ozaveščeni in motivirani, tehnologija je posodobljena, izvajajo se ustrezne meritve učinkovitosti, postopki so dokumentirani, predpisani in nadzorovani, kibernetske grožnje so na sprejemljivi ravni, ukrepi pa upoštevajo zahteve in potrebe uporabnikov ter poslovnih procesov. V resnici pa so takšne okoliščine

v realnem poslovnem okolju težko dosegljive, saj se poslovne razmere nenehno spreminjajo, naklonjenost vodstva varnostnemu področju stalno niha, spreminjajo pa se tudi struktura tehničnih oddelkov in njihove pristojnosti oz. odgovornosti. Tudi teoretične predpostavke in aktualne študije dokazujejo, da je trenutno stanje informacijske varnosti v organizacijskem okolju parcialno in le redko urejeno celovito oz. učinkovito.

Neustrezno stanje varnosti informacijskih sistemov ogroža splošno stanje varnosti poslovnega okolja, preživetje posameznih poslovnih entitet, v primeru uresničenih groženj pa se povečuje nestabilnost (nacionalnega) gospodarstva in zmanjšujejo možnosti za njegovo hitrejše okrevanje. Da bi v kontekstu trenutnih gospodarskih razmer in varnostnih trendov informacijsko varnost urejali v skladu s potrebami in z zmožnostmi organizacij ter prispevali k bolj varnemu poslovanju, je treba proučiti in razumeti pogoje, ki določajo, kdaj je (informacijska) varnost učinkovita.

2 UČINKOVITOST VARNOSTNE FUNKCIJE

Učinkovitost organizacijskih aktivnosti je temeljna poslovna potreba in cilj vsake sodobne organizacije (Mouzas, 2006; Computer crime and security survey,[1] 2011). Termin učinkovitost je tesno povezan s pojmoma uspešnost in odličnost, zaradi česar v praksi tovrstne izraze pogosto obravnavajo kot sinonime, z vidika organizacijskega okolja pa se pojavljajo v različnih kontekstih.

Evropska centralna banka navaja, da je ugotavljanje učinkovitosti upravljavskih nalog zelo zahtevna naloga, ki jo je veliko lažje izvesti in oceniti subjektivno kakor objektivno v obliki natančnih podatkov (Afonso, Schuknecht in Tanzi, 2006). Uspešnost z organizacijskega vidika pomeni stopnjo doseganja zastavljenih organizacijskih ciljev. Pri tem velja, da uspešno podjetje stalno napreduje in se razvija zaradi izpolnjevanja ciljev oz. interesov vodstvenega kadra. Učinkovitost v istem kontekstu pomeni povečevanje poslovne koristi oz. rezultata ob hkratnem zmanjševanju skupnega vložka oz. porabljenih virov (Vila, 1994). Organizacija je torej učinkovita, kadar poslovne rezultate ustvarja z najmanjšimi stroški, viri pa so učinkovito izkoriščeni, kadar z njihovo drugačno rabo ni mogoče bolje narediti niti ene dobrine, ne da bi pri tem naredili vsaj eno dobrino slabše[2] (Rebernik, 1994). Za ocenjevanje učinkovitosti morajo organizacije izpolniti tri pogoje: ocena stroškov, ocena koristi, primerjava stroškov in koristi. Iz tega sledi, da je za ocenjevanje učinkovitosti treba določiti izhodiščni položaj, ki ga lahko nadalje primerjamo s končnim stanjem (Afonso, Schuknecht in Tanzi, 2006). Pri analiziranju učinkovitosti je treba upoštevati, da sta pojma uspešnost in učinkovitost medsebojno neločljivo povezana in ju v organizacijskem okolju ni mogoče dosegati ali obravnavati ločeno.

Z uspešnostjo in učinkovitostjo lahko povežemo tudi koncept odličnosti podjetja, ki poleg stroškov in finančnih vidikov upošteva še druge odlike podjetja. Odličnost pomeni, da je podjetje pri poslovanju uspešno in ugledno v tolikšni meri, da postane močno konkurenčno in primer dobre prakse. Pri tem je treba upoštevati predvsem odnose med zaposlenimi, odnose do strank, vodstveno ozračje, vrednote podjetja in podjetniške taktike oz. inovativnost podjetja. Pri tem kot odlična podjetja označujemo tista, ki so sposobna v kompleksnem sistemu in okolju razviti preproste modele upravljanja in sprejemati hitre odločitve (Peters in Waterman, 1982). Če posplošimo, ukrepi so uspešni, kadar pripomorejo k doseganju organizacijskih ciljev, učinkoviti, kadar jih izpolnimo z minimalnimi investicijami, in odlični, kadar jih dosegamo preprosto in hitro, kar pripomore k razvoju, stabilnosti in ugledu organizacije. Težava, ki se pojavlja v organizacijah, je uskladitev zahtev po uspešnosti, učinkovitosti in odličnosti hkrati. V praksi organizacije pogosto stremijo samo k uspešnosti, torej doseganju zastavljenih ciljev, pri čemer velikokrat pozabljajo na dodano vrednost organizacijskega ugleda, zanemarjajo pa tudi merilo učinkovitosti oz. racionalno izpolnjevanje zahtev po uspehu (Mouzas, 2006).

Velike dileme pri ocenjevanju implementiranih ukrepov se pojavljajo predvsem v kontekstu varnosti, saj je varnost specifična organizacijska veja in področje, ki ga ni mogoče obravnavati in ocenjevati enako kot druge poslovne aktivnosti. O tem, kdaj je organizacija varna v celoti ali kdaj je varno njeno določeno področje, je zelo težko govoriti, saj je varnost abstraktno stanje, ki ga ni mogoče izraziti v natančnih in popolnoma objektivnih rezultatih. Trček (2006) navaja, da je varnost stanje minimalnih tveganj in da stanje absolutne varnosti ne obstaja, saj bodo vedno prisotna določena tveganja, ki jih ne moremo obvladati ali predvideti. Varnostna funkcija je v organizaciji podporne narave, saj omogoča nemo-

[1] Raziskava opravljena med 351 varnostnimi strokovnjaki, zadolženimi za informacijsko varnost v organizacijah.

[2] Z drugimi besedami: neki poslovni (lahko tudi varnostni) proces je učinkovit, kadar ne obstaja noben drug proces, ki bi ga lahko uporabili za proizvodnjo iste stopnje rezultata po nižjih stroških.

teno izvajanje vsakodnevnih poslovnih aktivnosti. Vsaka organizacija – še posebno v času gospodarske nestabilnosti – zahteva racionalnost pri razporejanju razpoložljivih virov za podporna področja, ki morajo prispevati k doseganju organizacijskih ciljev. Iz tega razloga mora biti varnost tako uspešna kakor tudi učinkovita.

Uspeh oz. izpolnjevanje postavljenih ciljev se na področju varnosti zato v relativno veliki meri povezuje z menedžersko-upravljavskimi funkcijami, kot so razvoj organizacije, načrtovanje in opredeljevanje organizacijskih ciljev, odzivanje na nepričakovane okoliščine, način in sposobnost vodenja, upravljanje s kadrovskimi viri, njihov razvoj in nadzor ter organizacijske vrednote. Pri tem je zelo pomembno, da organizacija določi in izbere pravo strategijo, kajti ukrepi so lahko uspešni, vendar še vedno neracionalni in neučinkoviti, kadar jih organizacija ne potrebuje in si pri tem zastavlja napačne cilje (Afonso, Schuknecht in Tanzi, 2006). Tudi Stewart (2012) navaja, da je upravljanje organizacije uspešno, kadar ima natančno določeno strategijo razvoja, načrt zagotavljanja varnosti pa je skladen z organizacijskimi cilji. Iz tega je razvidno, da so pogoji oz. merila ocenjevanja uspešnosti in učinkovitosti relativno nedoločeni in povezani z zelo abstraktnimi stanji, kar ustvarja veliko nejasnosti. Če zahteve po uspešnosti in učinkovitosti varnosti prenesemo na področje informacijske varnosti, je pri njunem pojasnjevanju in ocenjevanju treba upoštevati še nekatere specifične značilnosti omenjene funkcije.

2.1 Učinkovitost informacijske varnosti

Univerzalna in klasična definicija informacijske varnosti je zelo jedrnata in preprosta, saj po NIST-u (2013) »informacijska varnost pomeni zaščito informacij in informacijskih sistemov pred neavtoriziranim dostopom, uporabo, razkritjem, onemogočanjem ali uničenjem, z namenom zagotoviti njihovo zaupnost, celovitost in dostopnost«. Tudi organizacija ISO/IEC proces varovanja informacij opredeljuje kot ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij kakor tudi zagotavljanje drugih lastnosti, kot so verodostojnost, odgovornost, neovrgljivost in zanesljivost (ISO/IEC 27000: 2012).

V praksi si lahko organizacije pri doseganju omenjenih odlik informacijskega premoženja pomagajo z različnimi priročniki, navodili in standardi za organizacijsko upravljanje informacijske varnosti. V evropskem (in tudi svetovnem) prostoru so se uveljavila priporočila iz serije standardov ISO/IEC 27000 (Information security management system – ISMS), ki skupaj zajemajo celovit pristop k vzpostavljanju sistema upravljanja (ali vodenja) varovanja z informacijami (SUVI ali SVVI). Procesni model SUVI je natančno definiran in opisan v mednarodnem standardu ISO/IEC 27001: 2013,3 kontrole in praktična navodila za izpolnitev ciljev SUVI pa v standardu ISO/IEC 27002: 2013 (na voljo so npr. še ISO/IEC 27003: 2010 – vodnik za načrtovanje implementacije ISMS; ISO/IEC 27004: 2009 – metodologija za merjenje učinkovitosti SUVI; ISO/IEC 27005: 2011 – vodnik za proces upravljanja z informacijskimi tveganji, ISO/IEC 27006: 2011 – pogoji za izvajalce revizij in postopkov certificiranja, ISO/IEC 27007: 2011 – vodnik za ocenjevanje in revizijo upravljavskih procesov, ISO/IEC 27008: 2011 – vodnik za ocenjevanje ter revizijo varnostnih kontrol, ISO/IEC 27010: 2012 – vodnik za ocenjevanje kontrol medsektorskih in medorganizacijskih informacijskih sistemov, ISO/IEC 27011: 2008 – vodnik za informacijsko varnost telekomunikacijskih organizacij, ISO/IEC 27033: 2011 – priporočila pri načrtovanju in zagotavljanju varnosti omrežij idr.). Omenjeni standardi (v obliki priročnikov, kodeksov ali vodnikov) so namenjeni organizacijam in podjetjem, da z njihovo pomočjo dosežejo primerno informacijsko varnost in varnost poslovanja.

Področja, ki jih zajema in od organizacij zahteva krovni standard informacijske varnosti ISO/IEC 27000: 2013, so zaradi kompleksnosti poslovanja in vpliva mnogoterih dejavnikov na organizacijsko (informacijsko) varnost, številna in raznovrstna. To pomeni, da je tehnične kontrole nujno treba dopolnje-

[3] Oktobra 2013 je izšla prenovljena in posodobljena verzija standarda ISO/IEC 27001: 2013 (pred tem ISO/IEC 27001: 2005), ki je vsebino prilagodila najnovejšim tehnološkim in varnostnim trendom (spremembe in posodobitve se vsebinsko nanašajo na upoštevanje varnostnih vprašanj glede računalništva v oblaku, zunanjega izvajanja storitev, sodelovanja s tretjimi strankami – poudarek na dobaviteljih informacijsko-komunikacijske tehnologije, upoštevanje informacijske varnosti pri projektnem menedžmentu, omejitve pri nalaganju in uporabi programske opreme, varnostna načela pri sistemskem inženiringu, dostopnosti kritičnih poslovnih procesov itd.). Z organizacijskega vidika je sedaj obveznih 148 kontrolnih točk (pred tem 102), pri čemer so bolj poudarjeni postopki upravljanja – menedžment. Kljub temu je posodobljeni standard manj rigiden in bolj fleksibilen – organizacijam daje več manevrskega prostora pri sprejemanju odločitev o načinih izpolnjevanja obveznih kontrol. Nova verzija tako vsebuje 14 vsebinskih sklopov in 114 kontrol (stara 11 sklopov in 133 kontrol). Vsebinski sklopi v prenovljeni verziji standarda so: 1) menedžment informacijske varnosti, 2) organizacija informacijske varnosti, 3) varovanje človeških virov, 4) upravljanje s premoženjem, 5) nadzor dostopa, 6) kriptografija, 7) fizična in okoljska varnost, 8) varnost računalniških operacij, 9) komunikacijska varnost, 10) pridobivanje, razvoj in vzdrževanje informacijskih sistemov, 11) odnosi z dobavitelji, 12) upravljanje z incidenti, 13) neprekinjeno poslovanje, 14) skladnost (BSI Group, 2013).

vati z netehničnimi oz. upravljavskimi procesi, ustrezen menedžment pa je zato nujni pogoj učinkovitosti informacijske varnosti. ISO 27000: 2012 določa, da je organizacija pri zagotavljanju informacijske varnosti učinkovita, kadar so kontrole standarda (cilji) izpolnjene, obenem pa je zagotovljena sorazmernost med načinom doseganja ciljev in uporabljenimi viri.

Pomen upravljanja, nadzora in racionalnosti pri zagotavljanju informacijske varnosti izpostavlja tudi Ponemon Institute (Security effectiveness framework study, 2010), ki v primerjavi z ISO/IEC bolj splošno opredeljuje pogoje, ki morajo biti izpolnjeni za učinkovito informacijsko varnost v organizacijskem okolju. Organizacija mora:

1. biti sposobna preprečiti in hitro odkriti zunanje zlonamerne grožnje ter notranje zlorabe in napake,
2. biti odporna na varnostne incidente v obliki hitrega okrevanja in zagotavljanja neprekinjenega poslovanja,
3. zagotoviti skladnost postopkov in ukrepov z zahtevami zakonodaje in regulatorjev,
4. racionalno razporejati kadrovske in finančne vire,
5. izvajati dosleden nadzor nad upoštevanjem notranjih varnostnih pravil in postopkov.

Da bi lahko organizacije racionalno oz. gospodarno zagotovile čim bolj celovito obravnavo informacijske varnosti, morajo izpolniti enega izmed glavnih pogojev učinkovitosti – poznavanje dejanskega stanja ogroženosti in določanje prioritetnih varnostnih potreb, ki jih je treba nasloviti. Učinkovit pristop zavarovanja zaupnih informacij mora temeljiti na rezultatih analize tveganj in nadaljnjih analizah stroškov ter racionalnosti zaščitnih ukrepov. To najprej vključuje identifikacijo kritičnega informacijskega premoženja, njegove ranljivosti in grožnje. Na podlagi rezultatov takšne analize lahko organizacija v nadaljevanju izbira racionalne in učinkovite varnostne ukrepe glede na realno stanje ogroženosti (Sethuraman in Adaikkappan, 2009; Peláez, 2010). Pri tem bi morale organizacije, ki želijo zagotoviti optimalno varnost in racionalno razporejanje virov, najprej presoditi, katera področja je treba zaščititi ali varnostno posodobiti, in šele nato sprejemati odločitve, koliko virov bodo namenile za njihovo zaščito. V nasprotnem primeru, ko organizacije vnaprej določajo razpoložljive vire in jih šele nato razporejajo, so neracionalne odločitve zelo pogosta posledica. Varnostni ukrepi, ki jih ni mogoče upravičiti in pojasniti – torej argumentirati z zanesljivimi informacijami, so neracionalni in neučinkoviti (Stewart, 2012).

Med pogoje učinkovitosti informacijske varnosti spada tudi zahteva po sprejemanju dobrih kompromisov med varnostnimi in poslovnimi funkcijami oz. po ravnovesju med varnostjo in uporabnostjo informacijsko-komunikacijske tehnologije, ob hkratnem zagotavljanju zadostne stopnje zasebnosti uporabnikov. Koncept »organizacijski kompromis« se pri zagotavljanju informacijske varnosti nanaša na idejo, da je za pridobitev določene odlike sistema treba žrtvovati ali zmanjšati drugo odliko istega oz. drugega sistema/procesa (Wolter in Reinecke, 2010). Informacijskovarnostni ukrepi, ki so sicer uspešni pri preprečevanju groženj, ne morejo biti učinkoviti, kadar onemogočajo izvajanje poslovnih aktivnosti oz. kadar varnostni mehanizmi pretirano omejujejo funkcionalnost informacijsko-komunikacijske tehnologije in njenega namena (Johansson, 2004). Prav tako mora biti uporaba informacijskih sistemov omogočena na način, ki uresničuje pravice zaposlenih in varuje njihovo zasebnost, saj kršitve pravic uporabnikov nasprotujejo ciljem organizacije in splošnim zakonskim zahtevam (Conklin, White, Williams, Davis in Cothren, 2011). Kot pravi Anderson (2006), morajo organizacije določiti poslovne prioritete in nadrejene varnostne zahteve, ki jih je treba izpolniti, hkrati pa oceniti, katere odlike je zaradi tega mogoče zmanjšati in v kolikšni meri. Učinkovitost informacijske varnosti torej ni odvisna samo od uspeha posameznih varnostnih ukrepov (onesposobitev ali onemogočenje groženj), ki jih izbere organizacija, temveč od sprejemanja (dobrih) odločitev in kompromisov. Določeni ukrepi so lahko sicer uspešni in preprečujejo uresničitev neke grožnje, vendar so v določenem organizacijskem okolju nepotrebni. Ker je glede na nizko stopnjo ogroženosti organizacije njihova implementacija lahko moteča, se grožnja upravlja manj invazivno. V drugačnem, varnostnem okolju pa bi bila uporaba enakih ukrepov edini način zaščite oz. upravljanja tveganj (Schneier, 2008).

Iz vsega zapisanega je razvidno, da je informacijska varnost v organizacijskem okolju zelo obsežno področje, ki zahteva multidisciplinaren in timski pristop ter različne kompetence in sposobnosti varnostnih strokovnjakov (Thomson in Solms, 2006; Whitman in Mattord, 2008; Ivanc, 2013). V praksi se organizacije ravno zaradi kompleksnosti in heterogenosti področja pri optimizaciji varnosti informacij

in odpravljanju groženj srečujejo z različnimi dilemami. K temu močno pripomorejo tudi varnostni in poslovni trendi, s katerimi se soočajo vse sodobne organizacije.

3 VPLIV GOSPODARSKE KRIZE NA VARNOST

Organizacije v zadnjem desetletju ni zaznamoval samo tehnološki razvoj. Poslovne entitete se soočajo s splošno neugodnimi razmerami oz. s finančno krizo, ki vpliva na varnostne razmere in organizacijski obstoj v poslovnem okolju. Glede na trenutni gospodarski položaj je pri zagotavljanju učinkovitosti informacijske varnosti poleg varnostnih potreb treba upoštevati tudi zmogljivosti organizacij. Viri, ki jih ima trenutno na voljo povprečna organizacija, so omejeni. Peláez (2010) ugotavlja, da je ravno proračun informacijske varnosti glavna ovira učinkovitega urejanja tega področja.

Na splošno se vpliv finančne krize na varnost kaže v pomanjkanju finančnih virov, zmanjševanju stopnje varnosti, manjši stopnji splošne učinkovitosti organizacij in slabšem upravljanju procesov (TMT Global security study, 2011).[4] Analize vpliva krize na poslovno okolje kažejo, da sta bili s finančno krizo najbolj prizadeti likvidnost in finančna zmogljivost podjetij (OECD, 2009), zaradi česar se zmanjšujejo razpoložljivi finančni viri za zagotavljanje varnosti (Melese, 2009). Tudi slovensko poslovno okolje se je zaradi omenjene finančne krize znašlo v zelo neugodnem položaju. Leta 2011 je 43 odstotkov podjetij, ki je v tem času prenehalo s poslovanjem, to storilo iz finančnih razlogov (Rebernik, Tominc in Crnogaj, 2012). Leta 2012 se je Slovenija uvrstila na 58. mesto (od skupno 67) glede poslovnih in razvojnih priložnosti ter sposobnosti podjetij (Xavier, Kelley, Herrington in Vorderwulbecke, 2013), kar nakazuje na to, da se tudi slovenska podjetja srečujejo z visokimi finančnimi in poslovnimi omejitvami.

Čeprav ima trenutna kriza v ekonomskem, političnem in poslovnem okolju negativen vpliv na varnostne sposobnosti organizacij, pa prav zaradi nje naraščajo varnostne potrebe le-teh. Stranke in poslovni partnerji zahtevajo vse večjo zaupnost pri poslovanju, vse večja pa je tudi potreba po informacijah oz. želja po konkurenčni prednosti (Allen in Westby, 2007; Figliuzzi, 2012), kar povečuje agresivnost v medorganizacijski tekmovalnosti (Economic Intelligence Unit, 2012).[5] Raziskave ugotavljajo (PWC, 2009;[6] Global information security survey, 2012;[7] TMT Global security study, 2011; Global state of information security survey, 2013), da je informacijska varnost zaradi vpliva na finančno stabilnost organizacij postala ena izmed glavnih skrbi in prioritet organizacij, saj tveganja na tem področju stalno naraščajo. Nasprotno pa iste raziskave ugotavljajo, da se varnostne pomanjkljivosti oz. razhajanja med dejanskimi in želenimi varnostnimi razmerami poglabljajo, kar pretežno pripisujejo slabi varnostni zasnovi informacijsko-komunikacijske tehnologije, neustreznim postopkom in pomanjkljivim upravljanjem s človeškimi viri – uporabniki. Rezultati raziskave vpliva gospodarske krize na delovni odnos ljudi, njihovo etiko in splošno stanje informacijske varnosti so pokazali, da so v tem času močno narasle grožnje, povezane z industrijskim vohunjenjem in krajo zaupnih podatkov. Motivacija in priložnosti naraščajo med zaposlenimi in hekerji, ki jim pomanjkanje virov za zagotavljanje varnosti v organizacijah odpira nove možnosti za zlorabe (Fullbrook, 2009; Global state of information security survey, 2012[8]). Raziskave ugotavljajo, da je v težkih ekonomskih časih človek najpogostejši vzrok informacijskovarnostnih incidentov, saj povečan stres in občutek strahu pred izgubo službe povzroči, da se zaposleni pogosteje obnašajo deviantno (TMT Global security study, 2011). Pri tem zaposleni kot uporabniki postajajo glavna tarča storilcev kibernetske kriminalitete, saj ljudje pomenijo najšibkejši člen varnostnega sistema, prek katerega je mogoče zaobiti tehnično zaščito in najhitreje pridobiti dostop do zaupnih in varovanih organizacijskih področij.

Zaradi povečevanja tveganj in omejenih organizacijskih virov podjetja zahtevajo vse večjo učinkovitost varnostnih ukrepov (PWC, 2009; Vaish in Varma, 2010; Hall, Sarkani in Mazzuchi, 2011), investicije, vložene v področje varnosti pa morajo odgovorni prikazati s hitrimi in konkretnimi rezultati (Ashraf, 2005; Pironti, 2007). Ker informacijska varnost v primeru učinkovitosti daje rezultate v obliki neuresničenih groženj, jo je težko dokazati s konkretnimi

[4] Mednarodna raziskava, opravljena v 138 organizacijah.

[5] Mednarodna raziskava, izvedena med 352 pripadniki varnostnega menedžmenta o grožnjah podatkom.

[6] Raziskava, opravljena med 7.200 pripadniki najvišjega menedžmenta v 130 državah.

[7] Raziskava, izvedena med 1.836 pripadniki informacijskovarnostnega menedžmenta v 64 državah.

[8] Raziskava, opravljena med 9.600 pripadniki varnostnega menedžmenta iz 138 držav.

(finančnimi) podatki (Stewart, 2012). Iz tega razloga je varnost pogosto tisto organizacijsko področje, pri katerem najprej uvajamo in sprejemamo varčevalne ukrepe. Na drugi strani pa ravno varčevalni ukrepi v smislu zmanjševanja finančnih in kadrovskih virov slabšajo splošno stanje varnosti, saj se s tem povečujejo možnosti za uresničitev kibernetskih groženj (Burton in Stewart, 2009; Knopik in Zhan, 2010). To dokazujejo tudi aktualne raziskave, ki kljub visokemu pomenu informacijske varnosti potrjujejo visoko stopnjo prisotnosti kibernetskih groženj v organizacijskem okolju in neučinkovitost organizacij pri njihovem upravljanju.

4 TRENUTNO STANJE INFORMACIJSKE VARNOSTI

Finančna kriza in gospodarska nestabilnost sta z vidika informacijske varnosti za večino organizacij ustvarili paradoksalen položaj. Podjetja zaradi naraščajočih in vse bolj sofisticiranih kibernetskih groženj potrebujejo visoko stopnjo informacijske varnosti ob hkratnem zmanjševanju razpoložljivih virov, namenjenih za njeno zagotavljanje. Zahtevamo torej uspeh informacijsko varnostnih ukrepov z minimalnimi investicijami. Nasprotno pa je zaradi omenjenih izzivov to področje v poslovnem okolju pogosto neurejeno in tudi v stroki ni konsenza o tem, kaj sploh pomeni učinkovitost (informacijske) varnosti in kako jo optimalno ter racionalno urediti. Tako Vršec (2013) navaja, da je v gospodarskih družbah in organizacijah nasploh premalo znanja, volje, zavedanja, vnašanja primerov dobrih praks in finančnih virov, zaradi česar v praksi ne uporabljamo učinkovitih varnostnih mehanizmov. Enako ugotavljajo tudi raziskave o trenutnem globalnem stanju informacijske varnosti.

Raziskave kažejo močne razlike med stopnjo učinkovitosti informacijske varnosti v različnih poslovnih okoljih. Pri tem ocenjujejo, da je učinkovitost informacijske varnosti najbolj ogrožena in najslabša v manjših podjetjih in v organizacijah, ki ne razvijajo varnostnega menedžmenta, medtem ko na bi bilo v splošnem približno 35 odstotkov organizacij neučinkovitih pri zagotavljanju informacijske varnosti (Security effectiveness framework study, 2010).[9] V praksi 52 odstotkov organizacij neučinkovito razporeja tudi obstoječe vire (TMT Global security study, 2011), le osem odstotkov podjetij oz. varnostnega menedžmenta pa se vede varnostno odlično (Global state of information security survey, 2013). Splošno neučinkovitost organizacij pri vzpostavljanju informacijske varnosti najpogosteje povezujejo z neučinkovitim menedžmentom oz. neustrezno miselnostjo o odgovornosti za zagotavljanje varnosti, ki ostaja zelo tradicionalna, tehnično usmerjena (Pironti, 2007; Peláez, 2010). V organizacijah, ki nimajo ustreznega strokovnega znanja, velikokrat prevladuje mnenje, da je informacijska varnost pretežno odgovornost IT-oddelka v organizaciji (Ashraf, 2005). To dokazujejo tudi raziskave, ki ugotavljajo zanemarjanje področje varnostnega menedžmenta. Analiza 9.300 podjetij v 128 državah je pokazala, da ima le 42 odstotkov organizacij proaktivno informacijskovarnostno strategijo, medtem ko imajo preostale pomanjkljive varnostne načrte (ali pa jih sploh nimajo) in se na grožnje odzivajo pretežno reaktivno (Global state of information security survey, 2013). Še bolj zaskrbljujoč je sklep raziskave, ki ugotavlja, da bi 97 odstotkov od 855 zaznanih incidentov v letu 2011 lahko preprečili s preprostimi oz. z osnovnimi varnostnimi rešitvami (Data breach investigation report, 2012), ki pa jih organizacije ne razvijajo.

Opisani problemi in predstavljene varnostne dileme dokazujejo, da je učinkovitost informacijske varnosti najpogosteje ogrožena zato, ker organizacije v poizkusih sledenja hitremu razvoju informacijsko-komunikacijske tehnologije in tehničnim ukrepom pozabljajo na osnovne varnostne predpostavke in prispevek človeškega faktorja k varnostnemu stanju v organizaciji (Ashraf, 2005). Tehnični ukrepi ne morejo biti učinkoviti, kadar jih uporabniki ne upoštevajo in ne razumejo varnostnih pravil (Herath in Rao, 2009), zaradi česar sta potrebna varnostno ozaveščanje in vpletenost uporabnikov v varnostne procese organizacije. Spears in Barkhi (2010) sta ugotovila, da aktivna udeležba zaposlenih pri vzpostavljanju varnostnih ukrepov skupaj s programi ozaveščanja pomembno vpliva na dvig dejanske stopnje informacijske varnosti v organizaciji. Tudi NIST (Wilson in Hash, 2003) v svojih priporočilih navaja, da stanje ozaveščenosti zaposlenih vpliva na manjšo stopnjo informacijskih incidentov. Medtem so Talib, Clarke in Furnell (2010) s pomočjo raziskave prišli do ugotovitve, da ljudje večino znanja, povezanega z varno uporabo informacijsko-komunikacijske tehnologije pridobimo ravno v delovnem okolju.

[9] Mednarodna raziskava, opravljena na vzorcu 101 organizacije.

Programi izobraževanja in usposabljanja so torej še toliko bolj pomembni, saj v delovnem okolju pridobljeno znanje prenašamo na druga okolja zunaj organizacije. Bernik in Meško (2011) sta ob analizi zavedanja in dojemanja kibernetskih groženj med uporabniki interneta v Sloveniji ugotovila, da na splošno obstaja pomanjkanje ozaveščenosti o kibernetskih grožnjah in zakonodaji na tem področju.

Pri proučevanju trenutnega stanja informacijske varnosti v organizacijskem okolju je problematična tudi ugotovitev, da informacijsko varnost v organizacijah pogosto najbolj ogrožajo tisti, ki so odgovorni za njeno učinkovitost in so zgled vsem zaposlenim. To potrjujejo intervjuji s tristotimi strokovnjaki, odgovornimi za menedžment (informacijske) varnosti v različnih organizacijah, pri čemer je bilo ugotovljeno, da jih 42 odstotkov meni, da zanje ne veljajo varnostna pravila in postopki. Pri opravljanju svojih aktivnosti ne upoštevajo procesnih ukrepov zagotavljanja varnosti oz. jih ignorirajo, hkrati pa imajo dostop do zaupnih informacij (Perception of security awareness study, 2012). V primeru neupoštevanja pravil in neodgovornega vedenja vodstva takšnemu zgledu navadno sledijo tudi drugi zaposleni, zaradi česar varnostni ukrepi ne morejo doseči svojega namena. Ob predpostavki, da za zagotavljanje informacijske varnosti organizacije razpolagajo s povprečnimi tehničnimi rešitvami in da lahko na dejavnike iz zunanjega okolja vplivamo le v manjši meri, sta posameznik in njegovo vedenje med ključnimi dejavniki učinkovitosti informacijske varnosti v organizacijah.

Iz ugotovitev prikazanih raziskav lahko predpostavljamo, da organizacije na splošno niso učinkovite pri zagotavljanju celovite organizacijske varnosti, prav tako pa pogosto sprejemajo neracionalne odločitve in slabe organizacijske kompromise. V trenutnih gospodarskih razmerah, ko je propadanje organizacij vsesplošen trend, sta njihov obstoj in preživetje odvisna od preudarnih in učinkovitih odločitev. Te so na področju informacijske varnosti najbolj ogrožene zaradi paradoksalnega stanja na področju upravičevanja investicij in upravljanja varnostnih tveganj.

Odločitve o investicijah v varnostno področje so v domeni vodstvenega kadra, ki (tudi) informacijsko varnost zelo pogosto povezuje s finančno koristjo varnostnih ukrepov in z idejo, da je varnost strošek. Zaradi dejstva, da je težko oceniti korist in učinkovitost implementiranih varnostnih ukrepov oz. ugotoviti, koliko je organizacija pridobila s tem, da se nepoznane grožnje niso uresničile, redko izvajajo ustrezne postopke ugotavljanja dejanskega stanja (Centre for Internet Security [CIS], 2010). Ocenjevanje informacijske varnosti je temeljni pogoj, ki ga mora izpolniti vsaka organizacija, ki želi zagotoviti učinkovito informacijsko varnost. Gre za proces, s katerim ugotavljamo, v kolikšni meri so izpolnjeni cilji informacijskovarnostne politike (ki je tudi prvi pogoj za izvajanje merskih postopkov) in koliko ti cilji pripomorejo k celovitem stanju varnosti v organizaciji (SANS Institute, 2007). Slagell (2010) ugotavlja, da je analiziranje tveganj zelo redka organizacijska praksa, na podlagi katere bi organizacije sprejemale odločitve. Če pa že izvajajo tovrstne analize, so pri tem prepuščene same sebi in lastnemu (pogosto omejenemu) znanju, analize pa so medsebojno neenotne nedosledne in neprimerljive. Glede na dejstvo, da organizacije pogosto trpijo pomanjkanje strokovnega znanja, volje in finančnih virov, medtem ko so storitve varnostnih svetovalcev pogosto finančno prezahtevne, je omejeno poznavanje stanja logična posledica. To potrjujejo tudi študije, ki poročajo o stagnaciji poizkusov ocenjevanja informacijske varnosti v praksi (Mimoso, 2009). Raziskave ugotavljajo, da podjetja sicer aktivno razvijajo informacijsko varnost, vendar varnostne zmogljivosti podjetij nazadujejo od leta 2008, saj 65 odstotkov organizacij ne analizira stanja informacijske varnosti oz. je to ocenjevanje neučinkovito in neustrezno razvito (Global state of information security survey, 2012; Info Security, 2011). Pomanjkanje točnih in aktualnih informacij o trenutnem stanju varnosti in ogroženosti ali napačne informacije, ki so posledica neustreznih postopkov ugotavljanja dejanskega stanja, vodijo v nepravilne odločitve, ki temeljijo na predvidevanjih (Pironti, 2007). Zaradi pomanjkanja informacij o dejanskem stanju varnosti se podjetja na viktimizacijo v praksi najpogosteje odzivajo z odpravo posledic prvotne viktimizacije; s povečanjem fizične varnosti, zmanjšanjem privlačnosti tarče in nadzorom dostopa (Lamm Weisel, 2005; Global state of information security survey, 2013). Najpogosteje torej uporabljajo situacijsko prevencijo, najmanj pa v praksi uporabljajo socialno strategijo, s katero bi ugotavljali dejanske vzroke viktimizacije in poskušali uvajati dolgoročne spremembe, saj to zahteva veliko časa in truda.

4.1 Stanje kibernetske kriminalitete v organizacijskem okolju

Na splošno se organizacije nenehno srečujejo z različnimi notranjimi in zunanjimi tveganji, ki zajemajo grožnje poslovnemu uspehu, finančni stabilnosti in varnosti nasploh. Določene grožnje so v poslovnem okolju prisotne že dolgo časa, zaradi česar so se nekaterim bolj ali manj uspešno prilagodile in standardizirale postopke njihovega upravljanja. V primeru hitrega in nepričakovanega razvoja informacijsko-komunikacijske tehnologije in kibernetskih groženj pa veliko organizacij ni imelo časa ali znanja, da bi se ustrezno zaščitile in dosledno sledile trendom razvoja. Zaradi tega so se na različnih točkah organizacijske strukture pojavile številne varnostne vrzeli oz. ranljivosti (na ravni strojne in programske opreme, uporabnikov, podatkov in omrežja), prek katerih lahko dostopamo do najpomembnejšega organizacijskega premoženja. Kibernetske grožnje so postale sodobni vidik ogrožanja varnosti organizacij, saj ob njihovem uresničenju vsi drugi (klasični) varnostni ukrepi nimajo učinka. Pri tem je še posebno problematična kibernetska kriminaliteta, ki lahko z visoko stopnjo znanja in motivacije storilcev zaobide vse tehnične varnostne ukrepe in pridobi neposreden dostop do najpomembnejšega organizacijskega premoženja.

Učinkovitost informacijske varnosti mora biti prioriteta vsake organizacije, ki želi biti uspešna, saj kibernetske grožnje vztrajno naraščajo, gospodarske in druge družbe pa zaradi tega doživljajo vse več napadov na lastne informacijske sisteme (Global information security survey, 2012; Economic Intelligence Unit, 2012; Northcutt, 2012; Wilshusen, 2012; Vršec, 2013; Global state of information security survey, 2013). To dokazujejo tudi različne študije kibernetske kriminalitete. Podjetje Norton navaja, da naj bi bilo zaradi kibernetske kriminalitete na minuto oškodovanih več kot 140 žrtev (Cybercrime report, 2012), med katere uvrščamo tudi organizacije. Ob upoštevanju takšnega podatka lahko sklepamo, da je kibernetska kriminaliteta najbolj pogosta in razširjena grožnja, ki se lahko uresniči v vsakem organizacijskem okolju. Podjetje Symantec je leta 2011 analiziralo informacijskovarnostne incidente v dvesto državah in pri tem zabeležilo skupno 5,5 milijona zlonamernih napadov na informacijske sisteme. Dnevno so tako obravnavali 4.595 primerov, pri čemer je bilo vsak dan zaznanih povprečno 82 primerov napadov na organizacije. Takšni napadi so se zelo pogosto kazali v obliki t. i. »ciljanih napadov« z namenom vohunjenja za zaupnimi podatki (angl. ATP – advanced persistent threat), pri čemer gre za kombinacijo različnih groženj (npr. kombinacija socialnega inženiringa in zlonamerne programske opreme, vstavljene v informacijski sistem organizacije) (Internet security threat report, 2012). Isto podjetje je leta 2012 zaznalo 45-odstotno povečanje varnostnih incidentov, dnevno pa je obravnavalo 165 ciljanih napadov na podjetja (Internet security threat report, 2013). Po poročanju SI-CERT-a so se s takšnimi grožnjami leta 2012 soočala tudi slovenska podjetja, kar pomeni, da je trendu naraščajočih kibernetskih groženj izpostavljeno tudi slovensko poslovno okolje. Zaskrbljujoč je tudi podatek, da je omenjena organizacija v istem letu obravnavala več varnostnih incidentov kot v letih 2010 in 2011 skupaj (Poročilo o omrežni varnosti za leto 2012, 2013). Čeprav ugotovitve takšnih raziskav in viktimizacijskih študij niso popolnoma enotne, lahko iz podatkov upravičeno sklepamo, da so kibernetske grožnje stalno aktivne in pomenijo resno tveganje, ki ga podjetja ne smejo zanemarjati. To dokazuje tudi mednarodna študija, ki ocenjuje, da na tedenski ravni podjetja utrpijo približno dva uspešna kibernetska napada, na letni ravni pa se škoda zaradi teh v večjih korporacijah giba med enim in štirinajstimi milijoni dolarjev (v kar vključujemo tudi kvantitativno oceno posrednih posledic) (Cost of cyber crime study, 2012),[10] so pa posledice odvisne predvsem od vrste uresničene grožnje in velikosti podjetja (Security effectiveness framework study, 2010). Omenjene raziskave navajajo, da finančna škoda, povzročena z uresničenimi kibernetskimi grožnjami, iz leta v leto vztrajno narašča. Pri tem naj bi največje posledice zaradi tovrstne kriminalitete utrpela majhna in srednje velika podjetja, ki imajo v povprečju več kot štirikrat večje izdatke okrevanja kot večje organizacije. Manjša podjetja naj bi bila pogosteje podvržena kriminaliteti, povezani z zlonamerno programsko opremo, krajo informacijsko-komunikacijske tehnologije in zaupnih informacij, večja podjetja pa se najpogosteje srečujejo z bolj organiziranimi oblikami kibernetske kriminalitete, to so grožnje, povezane z notranjimi zlorabami, vdori prek spleta in DOS-napadi (Cost of cyber crime study, 2012; State of the

[10] Mednarodna raziskava o stroških informacijskovarnostnih incidentov, opravljena v 56 organizacijah.

endpoint,[11] 2013). Druga raziskava (Internet security threat report, 2012) ugotavlja, da je 50 odstotkov vseh napadov na podjetja usmerjenih v velike, druga polovica pa v manjše organizacije (pri tem so podjetja v velikosti od 1 do 250 zaposlenih tarča 18 odstotkov vseh zaznanih groženj zoper poslovno okolje).

Na splošno raziskave in viktimizacijske študije navajajo visoko stopnjo pogostosti kibernetske kriminalitete, vendar so takšne analize neenotne, nedosledne in komercialne narave, zato je njihove ugotovitve težko posploševati (Anderson idr., 2012; Sjouwerman, 2011). Kljub temu lahko iz ugotovitev prikazanih raziskav izoblikujemo splošen sklep, da so organizacije relativno neuspešne pri zoperstavljanju kibernetskim grožnjam. Podjetja imajo na trgu sicer na voljo veliko različnih varnostnih rešitev in storitev, s katerimi lahko upravljajo omenjene grožnje, vendar stalen razvoj in napredek na področju informacijsko-komunikacijske tehnologije za veliko organizacij ustvarja nepregleden položaj, v katerem je težko izbrati primerne in racionalne varnostne ukrepe.

4.2 Trendi na področju varnostnih storitev in tehnoloških novosti

Nepravilne odločitve, povezane z informacijsko varnostjo, so v praksi povezane s težnjo organizacij slediti tehnološkim in varnostnim trendom, ki pa niso nujno tudi najbolj učinkovita rešitev. Vprašanje o učinkovitosti se zelo pogosto pojavlja skupaj z vse pogostejšim prenosom odgovornosti za informacijsko varnost k tretjim specializiranim subjektom (zunanje izvajanje ali t. i. outsourcing varnostnih funkcij), prenašanjem podatkov v oblak in eksponentno integracijo mobilne tehnologije in z njimi povezanih aplikacij v delovne procese, česar se organizacije poslužujejo zaradi potrebe po optimizaciji stroškov (Markelj in Bernik, 2011; Järveläinen, 2012).

Zunanje izvajanje se v časih naraščajočih groženj in zahtev po učinkovitosti varnosti kaže kot najpogostejša praksa, ki se jo poslužuje varnostni menedžment v organizacijah, zadolžen za zagotavljanje informacijske varnosti. S tem se sicer določena tveganja prenesejo na zunanje organizacije in se posledično povečujejo druga tveganja in grožnje. Prenos varnostnih funkcij iz organizacijskega v zunanje okolje zelo pogosto vodi tudi v zmanjševanje delovne sile za zagotavljane informacijske varnosti znotraj organizacij, kar še posebno ogroža varnost zaupnega informacijskega kapitala, saj manj zaposlenih pomeni manj znanja in manj nadzora. Posledice tega se kažejo v povečani ranljivosti podjetij in večjih možnostih za napake (Fullbrook, 2009). Iz tega sledi, da se organizacije pri sprejemanju odločitev o vzpostavljanju varnostnega sistema ne smejo držati samo načela zniževanja stroškov in izogibanja odgovornosti, temveč morajo upoštevati prednosti investicij v lastne varnostne zmogljivosti, ki so neotipljive in nefinančne narave (Hriberšek in Ribič, 2013).

Poleg zunanjega izvajanja se organizacije vse pogosteje poslužujejo storitev računalništva v oblaku, pri čemer gre za prenos podatkov v oblak, s tem pa se zmanjšajo stroški informacijsko-komunikacijske tehnologije in vzdrževanja. Poleg pozitivnih strani takšnega ukrepa se vzporedno pojavlja vprašanje informacijske varnosti, saj ni natančno določeno, kdo lahko dostopa do informacij in kje natanko so locirani podatki oz. del oblaka s podatki (Markelj in Bernik, 2011). Takšne storitve zmanjšujejo nadzor nad dostopanjem in upravljanjem informacijskega kapitala. Informacije, shranjene v oblaku, so lahko brez vednosti lastnika dostopne različnim subjektom, zaradi česar je težko zagotoviti njihovo zaupnost in celovitost. Podatki so lahka tarča zlorabe avtoriziranih in neavtoriziranih dostopov, zainteresiranih tujih obveščevalnih in državnih služb, hekerjev oz. posameznih tehnično podkovanih zlonamernih storilcev (Thomson, 2011). Ker je poslovanje neke organizacije odvisno tudi od dobaviteljev, poslovnih partnerjev pogodbenih izvajalcev in navsezadnje tudi od konkurence, so sestavni del poslovnega informacijskega sistema tudi podatki teh zunanjih dejavnikov (Vršec, 2013). Zaradi tega je informacijska varnost v zunanjih, povezanih oz. partnerskih okoljih prav tako izjemno pomembna.

Poleg omenjenih trendov, ki povzročajo dileme na področju učinkovitosti informacijske varnosti, se kot problematično izpostavlja še eno področje. Kot napovedujejo raziskave, bodo v prihodnosti najnevarnejše kibernetske grožnje usmerjene tudi v ranljivost mobilne tehnologije (TMT Global security study, 2011; Internet security threat report, 2012), s katero organizacije skušajo poenostaviti delovne aktivnosti in postajajo vse bolj odvisne od nje. Znano je, da je mobilna informacijsko-komunikacijska tehnologija postala organizacijski trend, v trenutnem kontekstu pa je najmanj zaščitena in najbolj ranljiva.

[11] Raziskava, opravljena med 671 varnostnimi menedžerji velikih organizacij.

Njeni zaščiti zaradi razširjenosti in preproste uporabe, ki zmanjšujeta občutek tveganja, namenjajo izjemno malo pozornosti, tako z vidika politične ureditve kot tehnične zaščite (Global information security survey, 2012). Vse pogosteje je mogoče zaznati tudi t. i. trend BYOD,[12] ki še poglablja takšno stanje neustrezne zaščite. Gre za vnos osebne mobilne naprave, ki jo posameznik uporablja v zasebnem življenju, v organizacijo in delovno okolje za izpolnjevanje službenih obveznosti. To ustvarja položaj, v katerem se združujejo zasebne in poslovne aktivnosti uporabnika, kar povečuje možnosti za zlorabe in ranljivosti v organizacijski strukturi. Trendi razvoja kibernetske kriminalitete v prihodnosti kažejo, da se bodo grožnje razvile v smeri fokusiranih napadov na mobilne naprave zaposlenih, ki imajo dostop do korporativnega omrežja (Sjouwerman, 2012).

Iz opisanega je razvidno, da lahko poizkusi prilagajanja sodobnim varnostnim trendom in tehničnim novostim vodijo v povečane ranljivosti. To se navadno zgodi, kadar organizacije tega ne počno premišljeno in analitično ter novosti uvajajo na podlagi priporočil prodajalcev, ki imajo lahko dvomljive namene. Pri zagotavljanju učinkovitosti informacijske varnosti je zato v primeru načrtovanja in vzpostavljanja varnostnih načrtov treba upoštevati prednosti in slabosti sodobnih informacijskovarnostnih trendov in razumeti tveganja, ki jih povzroča implementacija takšnih ukrepov.

5 SKLEP

Analiza varnostnih trendov in pregled aktualnih raziskav o stanju kibernetske kriminalitete in splošne učinkovitosti informacijske varnosti potrjujejo predpostavko, da je informacijska varnost ena izmed najpomembnejših poslovnih funkcij, ki pa je hkrati najmanj razumljena in urejena. Razlogi neučinkovitega varnostnega stanja se nahajajo v različnih organizacijskih, osebnostnih in okoljskih dejavnikih. Na splošno ugotavljamo, da je učinkovita informacijska varnost pogojena s temi merili:

1. vodstvena podpora informacijski varnosti, ki podpira odprto komunikacijo in ima posluh za varnostne probleme;
2. (informacijsko)varnostna strategija, podprta z varnostno politiko, nad upoštevanjem katere se izvaja ustrezen nadzor;
3. zadostni finančni in kadrovski viri, ki omogočajo implementacijo osnovnih tehničnih rešitev;
4. odgovoren in usposobljen varnostni menedžment z ustrezno stopnjo avtoritete, ki razvija varnostno kulturo in daje pozitiven zgled zaposlenim;
5. ocenjevanje ogroženosti pred kibernetskimi grožnjami, prioritiziranje tveganj in ocenjevanje učinkovitosti izbranih varnostnih ukrepov;
6. skladnost varnostnih ukrepov z organizacijsko strategijo in minimalen vpliv na funkcionalnosti sistemov ter pravice in zasebnost uporabnikov;
7. analiziranje varnostnih trendov in preudarnost pri uvajanju tehnoloških novosti;
8. ozaveščanje zaposlenih o pravilih in postopkih ter motiviranje za pozitivno varnostno vedenje.

V prispevku predstavljene dileme, povezane z vzpostavljanjem informacijske varnosti, dokazujejo, da je izpolnjevanje zahteve po učinkovitosti izjemno zahtevna in problematična naloga varnostnega menedžmenta. Trenutno stanje v zunanjem poslovnem okolju, ki je zaznamovano s finančno nestabilnostjo, vse pogostejšimi varnostnimi tveganji in visoko potrebo po inovativnosti in konkurenčnosti, zahteva od organizacij drugačen pristop pri upravljanju varnosti, kot so ga te poznale v preteklosti. Vodstveni kader se mora pri tem zavedati, da je podpora varnostni funkcija nujna, saj uporaba informacijsko-komunikacijske tehnologije v prihodnosti ne bo upadla (trendi kažejo ravno nasprotno), prav tako pa lahko upravičeno pričakujemo nadaljnji razvoj groženj in tveganj. Prav tako se je treba zavedati, da zaradi heterogenosti in vpliva različnih dejavnikov ni mogoče informacijske varnosti urediti učinkovito na preprost in nenačrtovan način. Pri tem ni zadosti, da organizacije postopke le formalizirajo, temveč je pomembno, da procesi in pravila živijo tudi v praksi. Identificirati moramo tista področja, ki ne funkcionirajo tako, kot si želi menedžment ali vodstvo, in šele potem ustrezno ukrepati. Predvsem pa mora vsaka organizacija poiskati in tako poznati odgovor na dve temeljni vprašanji:

1. kakšno je trenutno varnostno stanje in
2. kakšen je načrt za prihodnost.

Kadar informacijsko varnost načrtujemo strateško in dolgoročno (kar je tudi pogoj njene učinkovitosti) mora odgovorni varnostni menedžment jasno in natančno določiti operativne, taktične in strateške varnostne cilje. Ti morajo biti argumentirani in temeljiti na točnih informacijah o aktualnih varnostnih ukre-

[12] »Bring your own device«.

pih ter njihovih vplivih na upravljanje ogroženosti. Tako lahko identificiramo stopnjo njihove kompatibilnosti s poslovnimi zahtevami in učinkovitosti ter identificiramo vrzeli, ki jih je treba urediti v prihodnosti. Organizacija mora vedeti, kaj si želi in iz kakšnega stanja bo izhajala pri doseganju ciljev. Želene varnostne razmere v prihodnosti pa morajo biti zastavljene racionalno in predvsem izvedljivo, saj lahko pretirana idealizem in optimizem – tako kot ravnodušnost in ignoranca – povečata varnostna tveganja. Poznavanje trenutnega varnostnega stanja, varnostnih potreb in zmogljivosti so torej nujni pogoji učinkovitosti informacijske varnosti. Podprti morajo biti z odprtimi komunikacijskimi kanali, ki preprečujejo pretirane enostranske in avtoritativne odločitve, saj je informacijska varnost multidisciplinarno področje, ki ni samo tehnične, temveč je tudi družboslovne in psihološke narave. Brez razumevanja omenjenih področij so neracionalne odločitve z običajno prekomernimi in nepotrebnimi ukrepi neizogibna posledica.

LITERATURA

[1] Afonso, A., Schuknecht, L. in Tanzi, V. (2006). *Public sector efficiency: Evidence for new EU member states and emerging markets.* Frankfurt: European central bank.

[2] Allen, J. H. in Westby, J. R. (2007). *Governing for enterprise security: Implementation guide US-CERT: Article 1 – Characteristics of effective security governance.* Pittsburg, PA: Carneige Mellon University.

[3] Anderson, A. (2006). Effective management of information security and privacy. *Educause Quartely, 6*(1), 15–20.

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T. in Savage, S. (2012). *Measuring the cost of cybercrime.* Pridobljeno na http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

[5] Ashraf, S. (2005). *Organization need and everyone's responsibility: Information security awareness – Global Information Assurance Certification Paper.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113.

[6] Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

[7] BSI Group. (2013). *Moving from ISO/EC 27001:2005 to ISOI/IEC 27001:2013.* Pridobljeno na http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf.

[8] Burton, S. in Stewart, S. (2009). *Security Implications of the global financial crisis.* Austin, TX: Stratfor Global intelligence. Pridobljeno na http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis.

[9] Centre for internet security [CIS]. (2010). *The CIS consensus security metrcis*. Pridobljeno na http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics.

[10] *Computer crime and security survey*. (2011). New York, NY: Computer Security Institute. Pridobljeno na http://gocsi.com/survey.

[11] Conklin, W. A., White, G., Williams, D., Davis, R. in Cothren, C. (2011). *CompTIA security*: *Certification guide*. Columbus, GA: McGraw-Hill.

[12] *Cost of cyber crime study: United States*. (2012). Traverse city, MI: Ponemon Instittute. Pridobljeno na http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[13] *Cybercrime report:* 2011. (2012). Mountain View, CA: Symantec. Pridobljeno na http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.

[14] *Data breach investigation report.* (2012). New York, NY: Verizon. Pridobljeno na http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[15] Economic Intelligence Unit. (2012). *Cyber theft of corporate intelectual proprety: The nature of the threat.* Pridobljeno na http://www.boozallen.com/media/file/Cyber-Espionage-Brochure.pdf.

[16] Figliuzzi, F. C. (2012). *Statement before the house committee on homeland security, subcommittee on counterterrorism and intelligence.* Federal Bureau of Investigation [FBI]. Pridobljeno na http://www.fbi.gov/news/testimony/economic-espionage-a-foreign-intelligence-threat-to-americans-jobs-and-homeland-security.

[17] Fullbrook, M. (2009). Tips on stamping out data leakage & industrial espionage during recession. *ICT Review: Computer Hardware and Software Review Journal.* Pridobljeno na http://ictreview.blogspot.com/2009/03/tips-on-stamping-out-data-leakage.html.

[18] *Global information security survey: Fighting to close the gap* (2012). London: Ernst&Young. Pridobljeno na http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf.

[19] *Global state of information security survey: Changing the game.* (2013). London: PWC. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf.

[20] *Global state of information security survey: Eye of the storm.* (2012). London: PWC. http://www.pwccn.com/webmedia/doc/634653330562192188_rcs_info_security_2012.pdf.

[21] Hall, J. H., Sarkani, S. in Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155–176.

[22] Herath, T. in Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision support systems, 47*(2), 154–165.

[23] Hriberšek, Z. in Ribič, A. (2013). Korporativna varnost kot konkurenčna prednost podjetja. *Korporativna varnost,* 2(3), 30–33.

[24] Info Security. (2011). *Most enterprises poor at measuring information security effectiveness.* Pridobljeno na http://www.infosecurity-magazine.com/view/16928/most-enterprises-poor-at-measuring-information-security-effectiveness/.

[25] *Internet security threat report*. (2012). Mountain View, CA: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17.

[26] *Internet security threat report.* (2013). Mountain View, CA: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[27] *ISO/IEC 27000: 2012.* (2012). Joint Technical Committe, JTC1. The International Organization for standardization and International Electotechnical Comission: Geneva.

[28] Ivanc, B. (2013). Varovanje občutljivih podatkov v informacijskih sistemih. V. I. Bernik in B. Markelj (ur.), *Sodobni aspekti informacijske varnosti*, str. 6–11. Ljubljana: Fakulteta za varnostne vede.

[29] Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships*. Information Management & Computer Security, 20*(5), 332–349.

[30] Johansson, J. M. (2004). *The fundamental tradeoffs. Microsoft security techcentre*. Pridobljeno na http://technet.microsoft.com/en-us/library/cc512573.aspx.

[31] Knopik, C. in Zhan, J. (2010). *The effects of financial crises on american financial institutions information security.* 5th conference on future information technology, 21.–23. 5. 2010. Madison, WI: Dakota state University.

[32] Lamm Weisel, D. (2005). *Analyzing repeat victimization.* Center for problem oriented policing: Tool guide No. 5. Pridobljeno na http://www.popcenter.org/tools/repeat_victimization/print/.

[33] Markelj, B. in Bernik, I. (2011). Mobilni dostop z vidika informacijske varnosti do podatkov v oblaku. T. P. Mrevlje in I. Areh (ur.), *Zbornik prispevkov 12. slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.uni-mb.si/dv2011/zbornik/informacijska_varnost/Markelj-Bernik-Oblak.pdf.

[34] Melese, F. (2009). *The financial crisis: a similiar effect to a terrorist attack.* NATO. Pridobljeno na http://www.nato.int/docu/review/2009/FinancialCrisis/Financial-terrorist-attack/EN/.

[35] Mimoso, M. S. (2009). *Number-driven risk metrics fundamentally broken.* Pridobljeno na http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#.

[36] Mouzas, S. (2006). Efficiency versus effectiveness in business networks. *Journal of Business Research, 59*(10–11), 1124–1132.

[37] NIST. (2013). *Glossary of key information security terms*. Gaithersburg, MD: NIST, U.S. Departement of Commerce.

[38] Northcutt, S. (2012). *Emerging trends in IT and security 2012 – 2014.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.sans.edu/research/security-laboratory/article/2012-emerging-trends.

[39] OECD. (2009). *OECD Strategic response to the financial and economic crisis.* Pridobljeno na http://www.oecd.org/economy/42061463.pdf.

[40] Peláez, M. H. S. (2010). *Measuring effectiveness in information security controls.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.sans.org/reading_room/whitepapers/basics/measuring-effectiveness-information-security-controls_33398.

[41] *Perception of security awareness study.* (2012). Gothenburg: Cryptzone. Pridobljeno na http://www.cryptzone.com/_download/articles/Cryptzone_Study_Perceptions_Security_Awareness.pdf.

[42] Peters, T. J. in Waterman, R. H. (1982). *In search of excellence: Lessons from America's best-run companies.* London: HarperCollins Publishers.

[43] Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal, 7*(2), str. 1–5.

[44] *Poročilo o omrežni varnosti za leto 2012*. (2013). Ljubljana: SI-CERT. Pridobljeno na http://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf.

[45] PWC. *(2009).Trial by fire: What global executives expect of information security in the middle of the world's worst economic downturn in thirty years*. London: PWC. Pridobljeno na http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1557.

[46] Rebernik, M., Tominc, P. in Crnogaj, K. (2012). *Usihanje podjetništva v Sloveniji.* GEM Slovenija 2011. Pridobljeno na http://www.gemslovenia.org/gem-porocila/.

[47] Rebernik, M. (1994). *Ekonomika podjetja*. Ljubljana: Gospodarski vestnik**.**

[48] SANS Institute. (2007). *A guide to security metrics.* Pridobljeno na http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

[49] Schneier, B. (2008). *The psychology of security*. Pridobljeno na http://www.schneier.com/essay-155.html.

[50] *Security effectiveness framework study.* (2010). Traverse city, MI: Ponemon Institute Pridobljeno na http://h71028.www7.hp.com/enterprise/downloads/software/Security%20Effectiveness%20Framework%20Study.pdf.

[51] Sethuraman, S. in Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. *ISACA Journal, 9*(5), str. 1–7.

[52] Sjouwerman, S. (2011). *Cyberheist: The biggest financial threat facing american since the meltdown in 2008*. Clearwater, FL: KNOWB4.

[53] Sjouwerman, S. (2012). 2013 security prediction. *Cyberheist News, 2*(54). Pridobljeno na http://blog.knowbe4.com/cyberheistnews-vol2-53/.

[54] Slagell, A. (2010). Thinking critically about computer security trade-offs. *Skeptical Inquirer.* Pridobljeno na http://www.csicop.org/si/show/thinking_critically_about_computer_security_trade-offs/.

[55] Spears, J. L. in Barkhi, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

[56] *State of the endpoint.* (2013). Traverse city, MI: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf.

[57] Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

[58] Talib, S., Clarke, N. L. in Furnell, S. M. (2010). *An analysis of information security awareness within home and work environments.* 5th International conference on availability, reliability and security: ARES 2010, 15.–18. 2. 2010 (str. 196–203). Cracow: IEEE computer soc. Pridobljeno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7348&context=ecuworks.

[59] Thomson, K. L. in Solms, R. (2006). Towards an information security competence maturity model. *Computer fraud&security, 18*(5), 11–15.

[60] Thomson, L. L. (2011). Cybercrime and escalating risks. V L. Thomson (ur.), *Data breach and encrypton handbook*, str. 3–16. Chicago, IL: American Bar Association Section of Science & Technology Law.

[61] *TMT Global security study: Raising the bar.* (2011). New York, NY: Deloitte. Pridobljeno na http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdfTrček, D. (2006). *Managing Infomation Systems Security and Privacy*. Berlin: Springer.

[62] Trček, D. (2006). *Managing Infomation Systems Security and Privacy*. Berlin: Springer.
[63] Vaish, A. in Varma, S. (2010). Parameter Extraction for Measurement of the Effective Information Security Management – Statistical Analysis. *International Journal of Computer and Electrical Engineering, 4*(2), 654–659.
[64] Vila, A. (1994). *Organizacija in organiziranje*. Kranj: Moderna založba.
[65] Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike varovanja informacij. *Korporativna varnost, 2*(3), 9–11.
[66] Whitman, M. E. in Mattord, H. J. (2008). *Management of information security*. Boston, MS: Course Technology Cengage Learning.
[67] Wilshusen, G. C. (2012). *Cyber threats facilitate ability to commit economic espionage.* NorthWest, WA: United states government accountability office, GAO. Pridobljeno na http://www.gao.gov/products/GAO-12-876T.
[68] Wilson, M. in Hash, J. (2003). *Building an information technology security awareness and training Program – NIST Special Publication 800-50.* Gaithersburg, MD: National Institute for standards and technology. Pridobljeno na http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
[69] Wolter, K. in Reinecke, P. (2010). Performance and security tradeoff. V A. Aldini, M. Bernardo, A. Di Pierro in H. Wiklicky (ur.), *Formal methods for quantitative aspects of programming languages*, 135–167. Berlin: Springer-Verlag.
[70] Xavier, S. R., Kelley, D., Herrington, K. J. in Vorderwulbecke, A. (2013). *2012 Global report.* Global enterpreneurship monitor. Pridobljeno na http://www.gemslovenia.org/news/.

▪

Kaja Prislan, mag. var., doktorska študentka na Fakulteti za varnostne vede, Univerza v Mariboru.

▪

Igor Bernik, docent in predstojnik katedre za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru.

VZGOJA IN IZOBRAŽEVANJE V INFORMACIJSKI DRUŽBI – VIVID 2014

Programski odbor vabi vse, ki želijo s svojimi izkušnjami in pogledi prispevati k reševanju problemov in odgovorom na vprašanja, ki jih prinaša informatizacija vzgojno-izobraževalnega procesa, da pošljejo prispevke v obsegu do 10 strani. Pripravljeni naj bodo v slovenskem, izjemoma v angleškem jeziku.

Pomembni datumi

- 7. julij 2014 – oddaja prispevkov
- 8. september 2014 – obvestilo avtorjem
- 22. september 2014 – oddaja končne, popravljene verzije prispevkov

Dodatne informacije so na voljo na spletni strani *http://vivid.fov.uni-mb.si* in po e-pošti: *mojca.bernik@fov.uni-mb.si*.